CLAIMS

Kindly amend the claims as follows.

1-28. (canceled)

29. (presently amended) A method for the secure initialization of mobile data carriers (IM) within the frame of an authorization system (A) ~~with application-specific or system-specific initialization data~~,

wherein said initialization data (DI, A-I, I-I) are generated in an authorization process in a secure environment (g) at a remote authorization authority (HA) by means of authorization means (AM)

said initialization data (DI) comprising authorization information (A-I) and initialization information (I-I), being application-specific or system-specific and being used to initialize a new data carrier, a new application (App3) or an extension of an application (App2.2).

and said initialization data are sent over a network (N) in a secure communication according to security rules corresponding to the authorization system

to a decentralized authorized read and write station (A-WR) in an unsecured environment (u),

where the mobile data carriers (IM) are initialized (IMj) with the initialization data (DI)

~~and/or that the initialization data (DI) are sent over the network (N) to a decentralized read and write station (WR), by means of which the read and write station is initialized (WRk) to put into operation new data carriers, new applications of extension of applications~~.

30. (canceled)

31. (previously presented) The method according to claim 29, wherein the authorization means (AM) are consisting of special authorization identification media (AM-IM) or of authorization data (AM-I).

32-37. (canceled)

38. (previously presented) The method according to claim 29, wherein with the initialization data (DI2.2) application extensions (App2.2) are initialized.

39. (previously presented) The method according to claim 29, wherein with the initialization data (DI3) new independent applications (App3) are initialized.

40. (previously presented) The method according to claim 29, wherein in a blank mobile data carrier which is prepared with a system data field (CDF) applications (App) are newly initialized with the initialization data (DI).

41. (canceled)

42. (previously presented) The method according to claim 29, wherein a connection between the authorization authority (HA) and the decentralized read and write stations (A-WR, WR) over the network (N) is only made occasionally and when an exchange of data takes place.

43. (previously presented) The method according to claim 29, wherein for the initialization a user authorization (aw) is effected by the read and write station (A-WR, WR), or by its owner (12) or an identification authorization means (ID-AM) is required.

44. (previously presented) The method according to claim 29, wherein for an initialization a user authorization (ai) by the data carrieror by the owner (13) of the data carrier takes place.

45. (previously presented) The method according to claim 29, wherein for the authorization of

initializations over the network (N), as well as for the execution of applications at the read and write station (A-WR, WR), at the data carrier (IM) personal data (aw) of the owner of the read and write station or personal data (ai) of the owner of the data carrier, are used as authorization means.

46. (previously presented) The method according to claim 29, wherein the mobile data carriers (IM) comprise an application micro-processor (AppuP) for the processing of application program data (I-I-Cod).

47. (previously presented) The method according to claim 29, wherein the data carriers (IM) are designed as contact-less, active or passive identification media.

48. (canceled)

49. (previously presented) The method according to claim 29, wherein status informations (S-I) concerning events at the authorized, or at the decentralized read and write stations (A-WR, WR) and/or at the mobile data carriers (IM) are sent to a corresponding authorization authority (HA) over the network (N).

50. (previously presented) The method according to claim 49, wherein the status informations (S-I) are utilized for usage or license fee debiting.

51-56. (canceled)

57. (presently amended) A mobile data carrier (IMj) for the communication with assigned decentralized read and write stations (WR, WRk)

within the frame of an authorization system (A), said mobile data carrier comprising

~~application-specific or system-specific~~ initialization data ~~(DI, A-I, I-I)~~ (DI), comprising authorization information (A-I) and initialization information (I-I).

~~to put into operation new data carriers, new applications or extension of applications~~

which are application-specific or system-specific and which are used to initialize the mobile data carrier (IMj), a new application (App3) or an extension of an application (App2.2),

wherein said initialization data (DI, A-I, I-I) were generated in an authorization process in a secure environment (g) at a remote authorization authority (HA) by means of authorization means (AM)

and said initialization data were sent over a network (N) in a secure communication according to security rules corresponding to the authorization system (A)

to a decentralized authorized read and write station (A-WR) in an unsecured environment (u)

and where the mobile data carrier was initialized (IMj) with said initialization data by said decentralized authorized read and write station (A-WR).

58. (presently amended) A read and write station (WRk) for the communication with assigned mobile data carriers (IM, IMj) within the frame of an authorization system (A), said read and write station comprising

~~application-specific or system-specific~~ initialization data ~~(DI, A-I, I-I)~~ (DI) comprising authorization information (A-I) and initialization information (I-I) ~~to put into operation new applications or extension of applications~~,

which are application-specific or system-specific and which are used to initialize a new application (App3) or an extension of an application (App2.2),

wherein said initialization data (DI, A-I, I-I) were generated in an authorization process in a secure environment (g) at a remote authorization authority (HA) by means of authorization means (AM)

and said initialization data were sent over a network (N) in a secure communication according to security rules corresponding to the authorization system (A)

to a decentralized read and write station (WR) in an unsecured environment (u)

by means of which said decentralized read and write station is initialized (WRk).

59. (presently amended) A method for the secure initialization of decentralized read and write stations (WR) within the frame of an authorization system (A) ~~with application-specific or system-specific initialization data~~,

wherein ~~said~~ initialization data ~~(DI, A-I, I-I)~~ (DI) and comprising authorization information (A-I) and initialization information (I-I) are generated in an authorization process in a secure environment (g) at a remote authorization authority (HA) by means of authorization means (AM)

said initialization data (DI, A-I, I-I) being application-specific or system-specific and being used to initialize a new application (App3) or an extension of an application (App2.2),

and said initialization data are sent over a network (N) in a secure communication according to security rules corresponding to the authorization system

to a decentralized read and write station (WR) in an unsecured environment (u), by means of which

said decentralized read and write station is initialized (WRk)~~, to put into operation new applications or extension of applications~~.

60. (previously presented) The method according to claim 59, wherein the authorization means (AM) are consisting of special authorization identification media (AM-IM) or of authorization data (AM-I).

61. (previously presented) The method according to claim 59, wherein a (non-authorized) decentralized read and write station (WR) at first is transformed into an authorized read and write station (A-WR) by means of function authorization data (A-I-FA) which are contained in the initialization data (DI), and which subsequently is capable of initializing mobile data carriers (IM) in correspondence with the initialization data.

62 (previously presented) The method according to claim 59, wherein a connection between the authorization authority (HA) and the decentralized read and write stations (A-WR, WR) over the network (N) is only made occasionally and when an exchange of data takes place.

63. (previously presented) The method according to claim 59, wherein for the initialization a user authorization (aw) is effected by the read and write station (A-WR, WR), or by its owner (12) or an identification authorization means (ID-AM) is required.

64. (previously presented) The method according to claim 59, wherein for the authorization of initializations over the network (N), as well as for the execution of applications at the read and write station (A-WR, WR), at the data carrier (IM) personal data (aw) of the owner of the read and write station or personal data (ai) of the owner of the data carrier, are used as authorization means.

65. (previously presented) The method according to claim 59, wherein the data carriers (IM) are designed as contact-less, active or passive identification media.

66. (previously presented) The method according to claim 59, wherein status informations (S-I)

concerning events at the authorized, or at the decentralized read and write stations (A-WR, WR) and/or at the mobile data carriers (IM) are sent to a corresponding authorization authority (HA) over the network (N).

67. (previously presented) The method according to claim 66, wherein the status informations (S-I) are utilized for usage or license fee debiting.